

# A Four-Round LOCC Protocol Outperforms All Two-Round Protocols in Reducing the Entanglement Cost for A Distributed Quantum Information Processing

Eyuri Wakakuwa\*

*Graduate School of Information Systems, The University of Electro-Communications, Japan*

Akihito Soeda and Mio Murao†

*Department of Physics, Graduate School of Science, The University of Tokyo, Japan*

(Dated: August 29, 2016)

We prove that there is a trade-off relation between the entanglement cost and the number of rounds of communication, for two distant parties to accomplish a bidirectional quantum information task by local operations and classical communication (LOCC). We consider an implementation of a class of two-qubit controlled-unitary gate by LOCC assisted by shared entanglement, in an information theoretical scenario of asymptotically many input pairs and vanishingly small error. We prove the trade-off relation by showing that one ebit of entanglement per pair is necessary to be consumed for implementing the unitary by any two-round protocol, whereas the entanglement cost by a four-round protocol is strictly smaller than one ebit per pair.

PACS numbers: 03.67.Bg, 03.67.Mn

## I. INTRODUCTION

When two distant parties collaborate to perform a distributed quantum information processing, it is necessary to communicate some information with each other. If the communication is restricted to be transmission of classical bits, it may also be necessary to make use of some entanglement shared in advance, depending on the task. Entanglement and classical communication are thus regarded as resources for distributed quantum information processing, and minimizing the cost of those resources has been one of the central issues in quantum information theory.

A relatively unexplored question about distributed quantum information processing is how the performance of a protocol to accomplish a task depends on the number of rounds of communication in the protocol [1]. It has been known that the performance of a protocol with more than one round of communication is strictly better than that of any protocol with only one round of communication, for several tasks such as entanglement distillation [2], quantum key distribution [3], state discrimination [4–6] and hypothesis testing [7–9]. However, few example of tasks is known for which an  $r'$ -round protocol outperforms any  $r$ -round protocol and  $2 \leq r < r'$ , with the exception of the result of [5]. Moreover, to our knowledge, it is not known whether there exists a trade-off relation between the entanglement cost and the number of rounds of a protocol for a “genuinely bidirectional” task, which cannot be accomplished by any protocol with only one round of communication.

In this paper, we investigate implementation of a bipar-

tite unitary gate by LOCC (local operations and classical communication) assisted by shared entanglement, in an information theoretical scenario introduced in [10]. We prove that, for a class of two-qubit controlled-unitary gates, a four-round protocol outperforms all two-round protocols in reducing the entanglement cost. Thus we provide a first example of genuinely bidirectional tasks for which there is a trade-off relation between the entanglement cost and the number of rounds of communication. It is different from the trade-off relation between the entanglement cost and the *classical communication cost*, which is known to exist, e.g., for remote state preparation [11–14].

This paper is organized as follows. In Section II, we introduce definitions of the problem. We present the main result and the proof in Section III. Conclusions are given in Section IV. Some technical parts of the proof of the main result are presented in Appendices.

*Notations.*  $|\Phi_d\rangle$ ,  $|\Phi_{K_n}\rangle$  and  $|\Phi_{L_n}\rangle$  represent the maximally entangled state with the Schmidt rank  $d, K_n, L_n \in \mathbb{N}$ , respectively.  $\pi_d$  is the maximally mixed state of rank  $d$ . The fidelity and the trace distance between two quantum states  $\rho$  and  $\sigma$  are defined as  $F(\rho, \sigma) := (\text{Tr}[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}])^2$  and  $\|\rho - \sigma\|_1 := \text{Tr}[\sqrt{(\rho - \sigma)^2}]$ , respectively. We abbreviate  $F(\rho, |\psi\rangle\langle\psi|)$  as  $F(\rho, |\psi\rangle)$ . For a quantum operation  $\mathcal{E}$ , we abbreviate  $\mathcal{E}(|\psi\rangle\langle\psi|)$  as  $\mathcal{E}(|\psi\rangle)$ .  $\log x$  represents the base 2 logarithm of  $x$ .

## II. DEFINITIONS

In this section, we describe a task that we analyze in this paper, and present a definition of a trade-off relation between the entanglement cost and the number of rounds.

Suppose Alice and Bob are given a sequence of bipartite quantum states  $|\psi_{i_1}\rangle^{AB} \cdots |\psi_{i_n}\rangle^{AB}$ , generated by

\*Electronic address: wakakuwa@quest.is.uec.ac.jp

†Also at Institute for Nano Quantum Information Electronics, The University of Tokyo, Japan

an i.i.d. quantum information source of an ensemble  $\{p_i, \psi_i\}_i$ . We assume that the source is completely mixed, i.e.,

$$\sum_i p_i |\psi_i\rangle\langle\psi_i|^{AB} = \pi_d^A \otimes \pi_d^B.$$

Alice and Bob perform the same bipartite unitary  $U^{AB}$  on each of  $|\psi_{i_1}\rangle^{AB}, \dots, |\psi_{i_n}\rangle^{AB}$  by LOCC using a resource state  $\Phi_{K_n}^{A_0 B_0}$ , in such a way that the average error vanishes in the limit of  $n \rightarrow \infty$ . Following the formulation of the Schumacher compression [15], we assume that Alice and Bob do not know the ensemble  $\{p_i, \psi_i\}_i$ , but know that the average state is completely mixed. An equivalent task is that Alice and Bob apply  $(U^{AB})^{\otimes n}$  on  $(|\Phi_d\rangle^{AR_A} |\Phi_d\rangle^{BR_B})^{\otimes n}$  by LOCC using a resource state  $\Phi_{K_n}^{A_0 B_0}$ . Here,  $R_A$  and  $R_B$  are imaginary reference systems that are inaccessible to Alice and Bob.

In general, a two-party LOCC protocol consists of concatenation of one party performing a local measurement and communicating a classical message to another. The number of concatenation is called the *number of rounds* of the protocol. For example, a two-round protocol proceeds as follows: Alice first performs a measurement and communicates the outcome to Bob; Bob then performs a measurement and communicates the outcome to Alice; and, finally, Alice performs an operation.

A rigorous definition of the entanglement cost of a unitary is given below.

*Definition 1* (Definition 1 in [10]) Let  $U$  be a bipartite unitary acting on two  $d$ -dimensional quantum systems  $A$  and  $B$ . Let Alice and Bob have quantum registers  $\{A_0, A_1\}$  and  $\{B_0, B_1\}$ , respectively, and let  $\mathcal{M}_n$  be a quantum operation from  $A^n A_0 \otimes B^n B_0$  to  $A^n A_1 \otimes B^n B_1$ .  $\mathcal{M}_n$  is called an  $(r, n, \epsilon)$ -protocol for implementing  $U$  if  $\mathcal{M}_n$  is an  $r$ -round LOCC that satisfies

$$F(\rho(\mathcal{M}_n), |\Psi_U\rangle^{\otimes n} |\Phi_{L_n}\rangle^{A_1 B_1}) \geq 1 - \epsilon, \quad (1)$$

where

$$|\Psi_U\rangle := U^{AB} |\Phi_d\rangle^{AR_A} |\Phi_d\rangle^{BR_B}$$

and

$$\rho(\mathcal{M}_n) := \mathcal{M}_n(|\Phi_d^{AR_A}\rangle^{\otimes n} |\Phi_d^{BR_B}\rangle^{\otimes n} |\Phi_{K_n}\rangle^{A_0 B_0}). \quad (2)$$

The entanglement cost of  $\mathcal{M}_n$  is defined by  $\log K_n - \log L_n$ .

*Definition 2* A rate  $E$  is said to be achievable by an  $r$ -round protocol for implementing  $U$  if, for any  $\epsilon > 0$ , there exists  $n_\epsilon$  such that for any  $n \geq n_\epsilon$ , we find an  $(r, n, \epsilon)$ -protocol for implementing  $U$  with the entanglement cost  $nE$ . For a technical reason, we additionally require that

$$\lim_{\epsilon \rightarrow 0} \epsilon \cdot n_\epsilon^4 = 0. \quad (3)$$

The entanglement cost of  $U$  by  $r$ -round protocols is defined as

$$E_r(U) := \inf\{E \mid E \text{ is achievable by an } r\text{-round protocol for implementing } U\}.$$

The main focus of this paper is whether there is a trade-off relation between the entanglement cost and the number of rounds for implementing a bipartite unitary. In considering “trade-off relation”, we compare the entanglement cost of a unitary by  $r$ -round protocols and that by an  $r'$ -round protocol ( $r < r'$ ). If the latter is strictly smaller than the former, we could say that there exists a trade-off relation between the entanglement cost and the number of rounds. A rigorous definition is as follows:

*Definition 3* There exists a trade-off relation between the entanglement cost and the number of rounds for implementing  $U$  if there exists  $r, r' \in \mathbb{N}$  such that

$$r < r', \quad E_r(U) > E_{r'}(U).$$

### III. RESULT AND PROOF

We consider a class of two-qubit controlled-phase gate, which takes the form of

$$U_\theta^{AB} = |0\rangle\langle 0|^A \otimes I^B + |1\rangle\langle 1|^A \otimes (e^{i\theta\sigma_z})^B$$

where

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad 0 < \theta \leq \frac{\pi}{2}.$$

The main result of this paper is as follows:

*Theorem 4* There exists a trade-off relation between the entanglement cost and the number of rounds for implementing  $U_\theta$  for any  $\theta \in (0, \theta_{\max}]$ , where  $\theta_{\max} \in (0, \pi/2]$  is a constant.

We prove Theorem 4 by showing that the following relations hold for any  $\theta \in (0, \theta_{\max}]$ :

$$E_2(U_\theta) \geq 1, \quad (4a)$$

$$E_4(U_\theta) < 1. \quad (4b)$$

Inequality (4a) is proved in [10] (see the converse part of Theorem 25 therein), and an outline of the proof will be presented at the end of this section. We prove Inequality (4b) in the following subsections, in which we also derive a stronger relation that

$$\lim_{\theta \rightarrow 0} E_4(U_\theta) = 0. \quad (5)$$

### A. A Single-Shot Four-Round Protocol

Let us first describe a single-shot protocol proposed in [16] for implementing the following two-qubit unitary gate by four-round LOCC:

$$\tilde{U}_\theta^{AB} = \cos\left(\frac{\theta}{2}\right) \cdot I^A \otimes I^B + i \sin\left(\frac{\theta}{2}\right) \cdot \sigma_z^A \otimes \sigma_z^B. \quad (6)$$

Note that  $\tilde{U}_\theta$  is equivalent to  $U_\theta$  up to local unitary transformations [17].

The protocol consists of a concatenation of two two-round protocols. In the first half, Alice and Bob implement  $\tilde{U}_\theta$  by using the following state as a shared resource (See Appendix A for the detail):

$$|\phi_\alpha\rangle^{A_0 B_0} = \cos\left(\frac{\alpha}{2}\right)|0\rangle|0\rangle + i \sin\left(\frac{\alpha}{2}\right)|1\rangle|1\rangle.$$

The protocol is probabilistic and the success probability is given by

$$p(\alpha, \theta) = \frac{\sin^2 \alpha}{2(1 - \cos \theta \cos \alpha)}$$

If the protocol succeeds,  $\tilde{U}_\theta$  is implemented on the input pair as desired, in which case Alice and Bob do nothing in the second half of the protocol. If it fails, then another controlled-unitary gate  $\tilde{U}_{\theta'}$  is applied to the input state. In that case, Alice and Bob continue to implement  $\tilde{U}_{\theta-\theta'}$  by a deterministic protocol proposed in [18] in the second half, which consumes one Bell pair. Note that  $\tilde{U}_{\theta-\theta'}\tilde{U}_{\theta'} = \tilde{U}_\theta$ . Thus the protocol succeeds in implementing  $\tilde{U}_\theta$  in total, regardless of the failure in the intermediate step. The average entanglement cost, measured by entanglement entropy, is given by

$$\bar{E}(\alpha, \theta) = 1 - p(\alpha, \theta) + h(\cos^2(\alpha/2)),$$

where  $h$  is the binary entropy defined by

$$h(x) := -x \log x - (1-x) \log (1-x).$$

Define

$$\alpha_\theta := \sqrt{\theta}, \quad p_\theta := p(\alpha_\theta, \theta), \quad E_\theta := \bar{E}(\alpha_\theta, \theta).$$

It is straightforward to verify that  $E_\theta$  is a continuous function of  $\theta \in (0, \pi/2]$ . As we prove in Appendix B 1, the function satisfies

$$\lim_{\theta \rightarrow 0} E_\theta = 0. \quad (7)$$

Thus there exists a constant  $\theta_{\max} \in (0, \pi/2]$  such that we have

$$E_\theta < 1 \quad (8)$$

for all  $\theta \in (0, \theta_{\max}]$ .

### B. An $n$ -Shot Protocol

Let us consider an  $n$ -shot protocol for implementing  $\tilde{U}_\theta$ . Fix arbitrary  $\delta > 0$  and  $n \in \mathbb{N}$ . The protocol proceeds as follows:

- I-1. Alice and Bob initially share  $n$  copies of  $|\phi_{\alpha_\theta}\rangle$  and  $n(1 - p_\theta + \delta)$  Bell pairs.
- I-2. By using  $n$  copies of  $|\phi_\alpha\rangle$  as resources, they perform  $\tilde{U}_\theta$  on each of the input sequence by the first half of the protocol described in Section III A. Either of the following two events will occur:
  - (a) The number of pairs for which  $\tilde{U}_\theta$  has been applied is not smaller than  $n(p_\theta - \delta)$ .  $\tilde{U}_{\theta'}$  has been applied on the other pairs, the number of which is not greater than  $n(1 - p_\theta + \delta)$ .
  - (b) The number of pairs for which  $\tilde{U}_\theta$  has been applied is smaller than  $n(p_\theta - \delta)$ .

Continue to the next step if (a) has occurred.

- I-3. By using  $n(1 - p_\theta + \delta)$  Bell pairs, they perform  $\tilde{U}_{\theta-\theta'}$  by the second half of the protocol described in Section III A, on pairs for which  $\tilde{U}_{\theta'}$  has been applied.

Let  $\mathcal{M}'_n$  be a quantum operation that represents Step I-2 and I-3, and suppose the input state is

$$|\Psi_n\rangle^{A^n B^n} := |\psi_1\rangle^{AB} \cdots |\psi_n\rangle^{AB}.$$

The total error is evaluated as follows. Let  $\epsilon_n$  be the probability that (b) occurs in Step I-2, and let  $\tau_{(b)}$  be the state obtained when (b) occurs. If (a) occurs in Step I-2, the final state is exactly equal to the target state  $|\Psi_{n,\text{tar}}\rangle := \tilde{U}^{\otimes n} |\Psi_n\rangle$ . Thus the final state is, in total, given by

$$\begin{aligned} \mathcal{M}'_n \left( |\Psi_n\rangle |\phi_{\alpha_\theta}\rangle^{\otimes n} |\Phi_2\rangle^{\otimes n(1-p_\theta+\delta)} \right) \\ = (1 - \epsilon_n) |\Psi_{n,\text{tar}}\rangle \langle \Psi_{n,\text{tar}}| + \epsilon_n \tau_{(b)}, \end{aligned}$$

which leads to

$$\begin{aligned} \left\| \mathcal{M}'_n \left( |\Psi_n\rangle |\phi_{\alpha_\theta}\rangle^{\otimes n} |\Phi_2\rangle^{\otimes n(1-p_\theta+\delta)} \right) \right. \\ \left. - \tilde{U}_\theta^{\otimes n} |\Psi_n\rangle \langle \Psi_n| \tilde{U}_\theta^{\dagger \otimes n} \right\|_1 \\ = \epsilon_n \left\| |\Psi_{n,\text{tar}}\rangle \langle \Psi_{n,\text{tar}}| - \tau_{(b)} \right\|_1 \leq 2\epsilon_n. \end{aligned} \quad (9)$$

The law of large numbers implies  $\lim_{n \rightarrow \infty} \epsilon_n = 0$ . It is proved in [19] that there exists an  $n$ -independent positive constant  $c_\theta$  such that

$$\epsilon_n \leq \exp(-c_\theta \delta^2 n) \quad (10)$$

for any  $\delta$  and  $n$ .

### C. Proof of Inequality (4b)

We prove that

$$E_4(U_\theta) \leq E_\theta \text{ for any } \theta \in (0, \pi/2].$$

This yields Inequality (4b) for  $\theta \in (0, \theta_{\max}]$  due to (8), as well as (5) due to (7). Note that the local unitary equivalence of  $U_\theta$  and  $\tilde{U}_\theta$  implies  $E_4(U_\theta) = E_4(\tilde{U}_\theta)$ . Thus we prove in the following that  $E_4(\tilde{U}_\theta) \leq E_\theta$  for any  $\theta \in (0, \pi/2]$ . We denote  $h(\cos^2(\alpha_\theta/2))$  simply by  $h_\theta$ .

Fix arbitrary  $\delta > 0$  and  $n \in \mathbb{N}$ , and consider the following protocol for implementing  $\tilde{U}_\theta$  with the entanglement cost  $n(E_\theta + 2\delta)$ .

- II-1. Alice and Bob initially share a maximally entangled state with Schmidt rank  $K_n = 2^{n(E_\theta + 2\delta)}$ .
- II-2. Alice and Bob transforms the resource entanglement to  $n(E_\theta + 2\delta)$  copies of Bell pairs by local unitary operations.
- II-3. By entanglement dilution [20], they transform  $n(h_\theta + \delta)$  copies of Bell pairs to a state  $\omega_n$  which is close to  $|\phi_{\alpha_\theta}\rangle^{\otimes n}$ .
- II-4. Alice and Bob perform  $\mathcal{M}'_n$  by using  $\omega_n$  and the remaining  $n(1 - p_\theta + \delta)$  Bell pairs as resource.

Let  $\mathcal{M}_n$  be a quantum operation that represents Step II-2~4, and define

$$\epsilon'_n := \left\| |\omega_n\rangle\langle\omega_n| - |\phi_{\alpha_\theta}\rangle\langle\phi_{\alpha_\theta}|^{\otimes n} \right\|_1. \quad (11)$$

By definition, we have

$$\mathcal{M}_n(|\Psi_n\rangle|\Phi_{K_n}\rangle) = \mathcal{M}'_n(|\Psi_n\rangle|\omega_n\rangle|\Phi_2\rangle^{\otimes n(1-p_\theta+\delta)}).$$

A simple calculation then yields

$$\left\| \mathcal{M}_n(|\Psi_n\rangle|\Phi_{K_n}\rangle) - \tilde{U}_\theta^{\otimes n}|\Psi_n\rangle\langle\Psi_n|\tilde{U}_\theta^{\dagger\otimes n} \right\|_1 \leq 2\epsilon_n + \epsilon'_n \quad (12)$$

from (9) (see Appendix B 2).

Since this relation holds for any  $|\Psi_n\rangle \in (\mathcal{H}^A \otimes \mathcal{H}^B)^{\otimes n}$ , it follows that

$$\left\| \mathcal{M}_n(|\Phi_2^{AR_A}\rangle^{\otimes n}|\Phi_2^{BR_B}\rangle^{\otimes n}|\Phi_{K_n}\rangle) - |\Psi_{\tilde{U}_\theta}\rangle\langle\Psi_{\tilde{U}_\theta}|^{\otimes n} \right\|_1 \leq 2\epsilon_n + \epsilon'_n.$$

As we prove in Appendix C, there exists an  $n$ -independent positive constant  $c'_\theta$  such that

$$\epsilon'_n \leq 2 \exp\left(-\frac{c'_\theta \delta^2 n}{2}\right) \quad (13)$$

for any  $\delta > 0$  and  $n \in \mathbb{N}$ . This ensures Condition (3) combined with (10), noting that the fidelity and the trace distance are related as  $F(\rho, \sigma) \geq 1 - \|\rho - \sigma\|_1$  (see e.g. [23]). Since  $\delta > 0$  can be arbitrarily small, we obtain  $E_4(\tilde{U}_\theta) \leq E_\theta$ . ■

### D. Outline of the Proof of Inequality (4a)

Let us first consider an arbitrary bipartite unitary  $U$  acting on two  $d$ -level systems  $A$  and  $B$ . Define a “tripartite” state

$$|\Psi_U\rangle^{AR_A(BR_B)} := (U^{AB} \otimes I^{RA RB})|\Phi_d\rangle^{AR_A}|\Phi_d\rangle^{BR_B}$$

by regarding  $B$  and  $R_B$  as a single system. Consider a task in which  $n$  copies of  $|\Psi_U\rangle^{AR_A(BR_B)}$  is transformed by a random unitary operation on  $A^n$  to a Markov state conditioned by  $B^n$ , i.e., a state that satisfies  $I(A^n : B^n R_B^n | R_A^n) = 0$  [21]. In particular, suppose  $2^{nR}$  unitary operations are randomly applied on  $A^n$  with the uniform distribution, and the trace distance between the final state and a Markov state vanishes in the limit of  $n \rightarrow \infty$ . The infimum ratio  $R$  satisfying this condition is called the *Markovianizing cost of  $U$* , and is denoted by  $M(U)$  [10, 22]. The following proposition states that  $M(U^\dagger)$  is a lower bound on the entanglement cost for implementing a bipartite unitary by a two-round protocol.

*Proposition 5* (Corollary of the converse part of Theorem 25 in [10]) A rate  $E$  is achievable by a two-round protocol for implementing  $U$  only if  $E \geq M(U^\dagger)$ , if we require Condition (3) in Definition 2.

The Markovianizing cost of a bipartite unitary is computed as follows. The *Petz recovery map*  $\mathcal{R}_U : A \rightarrow A(BR_B)$  corresponding to  $|\Psi_U\rangle^{AR_A(BR_B)}$  is defined by

$$\begin{aligned} \mathcal{R}_U(\tau) &= (\Psi_U^{A(BR_B)})^{\frac{1}{2}} (\Psi_U^A)^{-\frac{1}{2}} \tau (\Psi_U^A)^{-\frac{1}{2}} (\Psi_U^{A(BR_B)})^{\frac{1}{2}} \\ &= U^{AB} (\text{Tr}_B[U^{\dagger AB} (\tau^A \otimes I^B) U^{AB}]) \otimes \Phi_d^{BR_B} U^{\dagger AB} \end{aligned}$$

for  $\tau \in \mathcal{S}(\mathcal{H}^A)$  [21]. Define CPTP maps  $\mathcal{E}_U$  and  $\mathcal{E}_{U,\infty}$  on  $A$  by

$$\mathcal{E}_U := \text{Tr}_{BR_B} \circ \mathcal{R}_U, \quad \mathcal{E}_{U,\infty} := \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \mathcal{E}_U^n,$$

and consider the state

$$\Phi_{U,\infty}^{AR_A} := \mathcal{E}_{U,\infty}^A(|\Phi_d\rangle\langle\Phi_d|^{AR_A}).$$

It is proved in [10] that the Markovianizing cost of  $U$  is equal to the von Neumann entropy of  $\Phi_{U,\infty}^{AR_A}$ , i.e.,

$$M(U) = S(\Phi_{U,\infty}^{AR_A}).$$

For  $\tilde{U}_\theta$  defined by (6), we have

$$\mathcal{E}_{\tilde{U}_\theta^\dagger}(\tau) = \frac{1 + \cos^2 \theta}{2} \cdot \tau + \frac{1}{2} \sin^2 \theta \cdot \sigma_z \tau \sigma_z,$$

which leads to

$$\mathcal{E}_{\tilde{U}_\theta^\dagger, \infty}(\tau) = \frac{1}{2}(\tau + \sigma_z \tau \sigma_z) = |0\rangle\langle 0| \tau |0\rangle\langle 0| + |1\rangle\langle 1| \tau |1\rangle\langle 1|.$$

Hence we have

$$\Phi_{\tilde{U}_\theta^\dagger, \infty}^{AR_A} = \frac{1}{2}(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|),$$

which implies  $M(\tilde{U}_\theta^\dagger) = 1$ . Therefore, due to Proposition 5, we obtain Inequality (4a).

#### IV. CONCLUSION

We considered implementation of a class of two-qubit controlled-unitary gate by local operations and classical communication (LOCC), assisted by shared entanglement. We proved that a four-round protocol outperforms all two-round LOCC protocols in reducing the entanglement cost. Our result provides a first example of genuinely bidirectional distributed quantum tasks, for which there exists a trade-off relation between the entanglement cost and the number of rounds of communication.

#### Acknowledgments

This work is supported by the Project for Developing Innovation Systems of MEXT, Japan and JSPS KAKENHI (Grant No. 23540463, No. 23240001, No. 26330006, and No. 15H01677). We also gratefully acknowledge to the ELC project (Grant-in-Aid for Scientific Research on Innovative Areas MEXT KAKENHI (Grant No. 24106009)) for encouraging the research presented in this paper.

#### Appendix A: A probabilistic protocol for two-qubit controlled-unitaries

In this Appendix, we describe a protocol for implementing  $\tilde{U}_\theta$  by using resource state

$$|\phi_\alpha\rangle^{A_0 B_0} = \cos\left(\frac{\alpha}{2}\right)|0\rangle|0\rangle + i\sin\left(\frac{\alpha}{2}\right)|1\rangle|1\rangle,$$

which is proposed in [16]. Suppose the input state is  $|\psi\rangle^{AB}$ . The protocol proceeds as follows:

1. Alice performs the controlled- $z$  gate

$$U^{A_0 A} = |0\rangle\langle 0|^{A_0} \otimes I^A + |1\rangle\langle 1|^{A_0} \otimes \sigma_z^A,$$

after which the whole state is

$$\begin{aligned} |\psi'_{tot}\rangle^{A_0 B_0 AB} &= \cos\left(\frac{\alpha}{2}\right)|0\rangle^{A_0}|0\rangle^{B_0}|\psi\rangle^{AB} \\ &+ i\sin\left(\frac{\alpha}{2}\right)|1\rangle^{A_0}|1\rangle^{B_0}\sigma_z^A|\psi\rangle^{AB}. \end{aligned}$$

2. Alice performs a projective measurement on  $A_0$  with basis  $\{|+\rangle, |-\rangle\}$ , and sends the outcome to Bob.
3. Bob performs  $I$  or  $\sigma_z$  on  $B_0$  depending on the measurement outcome. The whole state is then

$$\begin{aligned} |\psi''_{tot}\rangle^{B_0 AB} &= \cos\left(\frac{\alpha}{2}\right)|0\rangle^{B_0}|\psi\rangle^{AB} \\ &+ i\sin\left(\frac{\alpha}{2}\right)|1\rangle^{B_0}\sigma_z^A|\psi\rangle^{AB}. \end{aligned}$$

4. Alice performs the controlled- $z$  gate

$$U^{B_0 B} = |0\rangle\langle 0|^{B_0} \otimes I^B + |1\rangle\langle 1|^{B_0} \otimes \sigma_z^B,$$

after which the whole state is

$$\begin{aligned} |\psi'''_{tot}\rangle^{B_0 AB} &= \cos\left(\frac{\alpha}{2}\right)|0\rangle^{B_0}|\psi\rangle^{AB} \\ &+ i\sin\left(\frac{\alpha}{2}\right)|1\rangle^{B_0}(\sigma_z^A \otimes \sigma_z^B)|\psi\rangle^{AB}. \end{aligned}$$

5. Bob performs a projective measurement on  $B_0$  with basis  $\{|\chi\rangle/\langle\chi|\chi\rangle^{1/2}, |\chi^\perp\rangle/\langle\chi^\perp|\chi^\perp\rangle^{1/2}\}$ , and sends the outcome to Alice. Here,  $|\chi\rangle$  and  $|\chi^\perp\rangle$  are supernormalized state vectors defined by

$$\begin{aligned} |\chi\rangle &:= \frac{\cos(\theta/2)}{\cos(\alpha/2)}|0\rangle + \frac{\sin(\theta/2)}{\sin(\alpha/2)}|1\rangle, \\ |\chi^\perp\rangle &:= \frac{\sin(\theta/2)}{\sin(\alpha/2)}|0\rangle - \frac{\cos(\theta/2)}{\cos(\alpha/2)}|1\rangle. \end{aligned}$$

If the measurement outcome corresponding to  $|\chi\rangle$  is obtained, the state becomes

$$\begin{aligned} |\psi^s\rangle^{AB} &= \langle\chi|\psi'''_{tot}\rangle \\ &= \cos\left(\frac{\theta}{2}\right)|\psi\rangle^{AB} + i\sin\left(\frac{\theta}{2}\right)(\sigma_z^A \otimes \sigma_z^B)|\psi\rangle^{AB} \end{aligned}$$

as desired. The success probability is given by

$$p(\alpha, \theta) = \frac{|\langle\chi|\psi'''_{tot}\rangle|^2}{\langle\chi|\chi\rangle} = \frac{1}{\langle\chi|\chi\rangle} = \frac{\sin^2 \alpha}{2(1 - \cos \theta \cos \alpha)}.$$

If the complementary outcome is obtained, then the state changes

$$\begin{aligned} |\psi^f\rangle^{AB} &= \langle\chi^\perp|\psi'''_{tot}\rangle \\ &= \frac{\sin(\theta/2)}{\tan(\alpha/2)}|\psi\rangle^{AB} + i\frac{\cos(\theta/2)}{\tan(\alpha/2)^{-1}}(\sigma_z^A \otimes \sigma_z^B)|\psi\rangle^{AB}, \end{aligned}$$

up to normalization condition. It is straightforward to verify that the normalized state satisfies

$$\frac{|\psi^f\rangle^{AB}}{\| |\psi^f\rangle^{AB} \|} = \tilde{U}_{\theta'}|\psi\rangle^{AB}$$

with  $\theta'$  defined by

$$\tan\left(\frac{\theta'}{2}\right) = \frac{\tan^2(\alpha/2)}{\tan(\theta/2)}.$$

#### Appendix B: Proof of Equality (7) and Inequality (12)

##### 1. Equality (7)

By definition, we have

$$\begin{aligned} E_\theta &= 1 - p_\theta + h(\cos^2(\sqrt{\theta}/2)), \\ p_\theta &= \frac{\sin^2 \sqrt{\theta}}{2(1 - \cos \theta \cos \sqrt{\theta})}. \end{aligned} \tag{B1}$$

It is straightforward to verify that

$$\lim_{\theta \rightarrow 0} h(\cos^2(\sqrt{\theta}/2)) = 0. \quad (\text{B2})$$

For  $\theta \approx 0$ , we have

$$\begin{aligned} \sin^2 \sqrt{\theta} &= \theta + O(\theta^2), \\ \cos \theta &= 1 - \frac{1}{2}\theta^2 + O(\theta^4), \\ \cos \sqrt{\theta} &= 1 - \frac{1}{2}\theta + O(\theta^2), \\ \cos \theta \cos \sqrt{\theta} &= 1 - \frac{1}{2}\theta + O(\theta^2). \end{aligned}$$

Thus we have

$$p_\theta = \frac{\theta + O(\theta^2)}{2(\frac{1}{2}\theta + O(\theta^2))} = 1 + O(\theta),$$

which leads to

$$\lim_{\theta \rightarrow 0} p_\theta = 1. \quad (\text{B3})$$

From (B1), (B2) and (B3), we obtain (7).  $\blacksquare$

## 2. Inequality (12)

We obtain Inequality (12) as

$$\begin{aligned} & \left\| \mathcal{M}_n(|\Psi_n\rangle|\Phi_{K_n}\rangle) - \tilde{U}_\theta^{\otimes n} |\Psi_n\rangle\langle\Psi_n| \tilde{U}_\theta^{\dagger \otimes n} \right\|_1 \\ &= \left\| \mathcal{M}'_n(|\Psi_n\rangle|\omega_n\rangle|\Phi_2\rangle^{\otimes n(1-p_\theta+\delta)}) \right. \\ & \quad \left. - \tilde{U}_\theta^{\otimes n} |\Psi_n\rangle\langle\Psi_n| \tilde{U}_\theta^{\dagger \otimes n} \right\|_1 \\ &\leq \left\| \mathcal{M}'_n(|\Psi_n\rangle|\omega_n\rangle|\Phi_2\rangle^{\otimes n(1-p_\theta+\delta)}) \right. \\ & \quad \left. - \mathcal{M}'_n(|\Psi_n\rangle|\phi_{\alpha_\theta}\rangle^{\otimes n}|\Phi_2\rangle^{\otimes n(1-p_\theta+\delta)}) \right\|_1 \\ & \quad + \left\| \mathcal{M}'_n(|\Psi_n\rangle|\phi_{\alpha_\theta}\rangle^{\otimes n}|\Phi_2\rangle^{\otimes n(1-p_\theta+\delta)}) \right. \\ & \quad \left. - \tilde{U}_\theta^{\otimes n} |\Psi_n\rangle\langle\Psi_n| \tilde{U}_\theta^{\dagger \otimes n} \right\|_1 \\ &\leq \left\| |\Psi_n\rangle\langle\Psi_n| \otimes |\omega_n\rangle\langle\omega_n| \otimes |\Phi_2\rangle\langle\Phi_2|^{\otimes n(1-p_\theta+\delta)} \right. \\ & \quad \left. - |\Psi_n\rangle\langle\Psi_n| \otimes |\phi_{\alpha_\theta}\rangle\langle\phi_{\alpha_\theta}|^{\otimes n} \otimes |\Phi_2\rangle\langle\Phi_2|^{\otimes n(1-p_\theta+\delta)} \right\|_1 \\ & \quad + 2\epsilon_n \\ &= \left\| |\omega_n\rangle\langle\omega_n| - |\phi_{\alpha_\theta}\rangle\langle\phi_{\alpha_\theta}|^{\otimes n} \right\|_1 + 2\epsilon_n \\ &= \epsilon'_n + 2\epsilon_n. \end{aligned}$$

Here, the first line follows from the definition of  $\mathcal{M}'_n$ ; the second line due to the triangle inequality for the trace distance; the third line from the monotonicity of the trace distance and Inequality (9); the forth line because we have  $\|\rho \otimes \tau - \sigma \otimes \tau\|_1 = \|\rho - \sigma\|_1$ ; and the fifth line from Inequality (11).  $\blacksquare$

## Appendix C: Proof of Inequality (13)

### 1. Typical Subspace

Define

$$\lambda_0 = \cos^2\left(\frac{\alpha_\theta}{2}\right), \quad \lambda_1 = \sin^2\left(\frac{\alpha_\theta}{2}\right),$$

and fix arbitrary  $\delta > 0$ ,  $n \in \mathbb{N}$ . A sequence  $\mathbf{x} = (x_1, \dots, x_n) \in \{0, 1\}^n$  is said to be  $\delta$ -weakly typical with respect to  $\{\lambda_x\}_{x \in \{0,1\}}$  if it satisfies

$$2^{-n(H(\{\lambda_x\})+\delta)} \leq \prod_{i=1}^n \lambda_{x_i} \leq 2^{-n(H(\{\lambda_x\})-\delta)}. \quad (\text{C1})$$

Here,  $H(\{\lambda_x\})$  is the Shannon entropy of a probability distribution  $\{\lambda_x\}_{x \in \{0,1\}}$  defined by

$$H(\{\lambda_x\}) := - \sum_{x \in \{0,1\}} \lambda_x \log \lambda_x,$$

and is equal to  $h_\theta$ . The set of all  $\delta$ -weakly typical sequences is called the  $\delta$ -weakly typical set, and is denoted by  $\mathcal{T}_{n,\delta}$ . The  $\delta$ -weakly typical subspace of  $(\mathcal{H}^{A_0})^{\otimes n}$  with respect to  $\phi_{\alpha_\theta}^{A_0} = \text{Tr}_{B_0}[|\phi_{\alpha_\theta}\rangle\langle\phi_{\alpha_\theta}|^{A_0 B_0}]$  is defined as

$$\mathcal{H}_{n,\delta} :=$$

$$\text{span} \{ |x_1\rangle \cdots |x_n\rangle \in (\mathcal{H}^{A_0})^{\otimes n} \mid (x_1, \dots, x_n) \in \mathcal{T}_{n,\delta} \}.$$

Let  $\Pi_{n,\delta}$  be the projection onto  $\mathcal{H}_{n,\delta} \subseteq (\mathcal{H}^{A_0})^{\otimes n}$ , and let us introduce a notation

$$\lambda_{\mathbf{x}} := \lambda_{x_1} \cdots \lambda_{x_n}.$$

Abbreviating  $(\Pi_{n,\delta} \otimes I_{B_0}^{B_0^n})|\phi_{\alpha_\theta}\rangle^{\otimes n}$  as  $\Pi_{n,\delta}|\phi_{\alpha_\theta}\rangle^{\otimes n}$ , we have

$$\text{Tr}[\Pi_{n,\delta}(|\phi_{\alpha_\theta}\rangle\langle\phi_{\alpha_\theta}|^{\otimes n})] = \sum_{\mathbf{x} \in \mathcal{T}_{n,\delta}} \lambda_{\mathbf{x}}. \quad (\text{C2})$$

It is proved in [19] that there exists a constant  $c > 0$ , which depends on  $\{\lambda_x\}_x$ , such that for any  $\delta > 0$  and  $n$ , we have

$$\sum_{\mathbf{x} \in \mathcal{T}_{n,\delta}} \lambda_{\mathbf{x}} \geq 1 - \exp(-c\delta^2 n).$$

Denoting this constant by  $c'_\theta$ , we obtain

$$\text{Tr}[\Pi_{n,\delta}(|\phi_{\alpha_\theta}\rangle\langle\phi_{\alpha_\theta}|^{\otimes n})] \geq 1 - \exp(-c'_\theta \delta^2 n)$$

from (C2).

### 2. Proof of Inequality (13)

Fix arbitrary  $\delta > 0$ ,  $n \in \mathbb{N}$ , and consider the normalized state  $|\omega_n\rangle$  defined by

$$|\omega_n\rangle := \frac{\Pi_{n,\delta}(|\phi_{\alpha_\theta}\rangle^{\otimes n})}{\sqrt{\text{Tr}[\Pi_{n,\delta}(|\phi_{\alpha_\theta}\rangle\langle\phi_{\alpha_\theta}|^{\otimes n})]}}. \quad (\text{C3})$$

Due to the gentle measurement lemma (see e.g. Lemma 9.4.1 in [23]), the state satisfies

$$\| |\omega_n\rangle\langle\omega_n| - |\phi_{\alpha_\theta}\rangle\langle\phi_{\alpha_\theta}|^{\otimes n} \|_1 \leq 2 \exp\left(-\frac{c'_\theta \delta^2 n}{2}\right).$$

By definition, the Schmidt decomposition of  $|\omega_n\rangle$  is given by

$$|\omega_n\rangle = \sum_{\mathbf{x} \in \mathcal{T}_{n,\delta}} \sqrt{\lambda'_\mathbf{x}} |\mathbf{x}\rangle |\mathbf{x}\rangle,$$

where

$$\lambda'_\mathbf{x} := \frac{\lambda_\mathbf{x}}{\text{Tr}[\Pi_{n,\delta}(|\phi_{\alpha_\theta}\rangle\langle\phi_{\alpha_\theta}|^{\otimes n})]}.$$

From (C1), it follows that

$$\lambda'_\mathbf{x} \geq 2^{-n(H(\{\lambda_x\})+\delta)}.$$

Thus a uniform distribution on a set  $\{1, \dots, 2^{n(H(\{\lambda_x\})+\delta)}\}$  is majorized by a probability distribution  $\{\lambda'_\mathbf{x}\}_{\mathbf{x} \in \mathcal{T}_{n,\delta}}$ . Consequently, due to [24], there exists a LOCC protocol that transforms  $n(H(\{\lambda_x\}) + \delta)$  copies of Bell pairs to  $|\omega_n\rangle$  deterministically and exactly. ■

- 
- [1] E. Chitambar, D. Leung, L. Mancinska, M. Ozols, and A. Winter, *Comm. Math. Phys.* **328**, 303 (2014).
  - [2] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Phys. Rev. A* **54**, 3824 (1996).
  - [3] D. Gottesman and H.-K. Lo, *IEEE Trans. Inf. Theory* **49**, 457 (2003).
  - [4] S. M. Cohen, *Phys. Rev. A* **75**, 052313 (2007).
  - [5] Y. Xin and R. Duan, *Phys. Rev. A* **77**, 012315 (2008).
  - [6] M. Owari and M. Hayashi, *New J. of Phys.* **10**, 013006 (2008).
  - [7] M. Owari and M. Hayashi, *IEEE Trans. Inf. Theory* **61**, 6995 (2010).
  - [8] M. Owari and M. Hayashi, *Phys. Rev. A* **90**, 032327 (2014).
  - [9] M. Owari and M. Hayashi, e-print arXiv:1409.3897v3.
  - [10] E. Wakakuwa, A. Soeda, and M. Murao, e-print arXiv:1505.04352v2.
  - [11] C. H. Bennett, P. Hayden, D. W. Leung, P. W. Shor, and A. Winter, *IEEE Trans. Inf. Theory* **51**, 56 (2005).
  - [12] A. Abeyesinghe and P. Hayden, *Phys. Rev. A* **68**, 062319 (2003).
  - [13] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, and J. A. Smolin, *Phys. Rev. Lett.* **87**, 077902 (2001).
  - [14] I. Devetak and T. Berger, *Phys. Rev. Lett.* **87**, 197901 (2001).
  - [15] B. Schumacher, *Phys. Rev. A* **51**, 2738 (1995).
  - [16] M.-Y. Ye, Y.-S. Zhang, and G.-C. Guo, *Phys. Rev. A* **73**, 032337 (2006).
  - [17] B. Kraus and J. I. Cirac, *Phys. Rev. A* **63**, 062309 (2001).
  - [18] J. Eisert, K. Jacobs, P. Papadopoulos, and M. Plenio, *Phys. Rev. A* **62**, 052317 (2000).
  - [19] R. Ahlswede, *J. Comb., Info. and Syst. Sciences* **5**, 10 (1980).
  - [20] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, *Phys. Rev. A* **53**, 2046 (1996).
  - [21] P. Hayden, R. Jozsa, D. Petz, and A. Winter, *Comm. Math. Phys.* **246**, 359 (2004).
  - [22] E. Wakakuwa, A. Soeda, and M. Murao, e-print arXiv:1504.05805v3.
  - [23] M. Wilde, *Quantum Information Theory* (Cambridge University Press, 2013).
  - [24] M. A. Nielsen, *Phys. Rev. Lett.* **83**, 436 (1999).